The Dudley Group
NHS Foundation Trust

Date: 21/12/2018

FREEDOM OF INFORMATION REQUEST 014493 – IT – shadow or feral systems

Under the provisions of the FOI Act, we request answers to the following questions:
• Does your Trust have a policy relating to shadow IT and feral systems. If yes, can you provide a copy of that policy?
• Has your Trust carried out a recent audit of shadow IT and feral systems?
• If Yes, can we have a copy of that audit? If No, will you provide an estimate of the number of such systems in your Trust?
• If you are unable to identify ALL shadow IT and feral systems, will you explain how you intend to meet your obligations under GDPR?
• Do you have a picture of how many feral systems adhere to NHS national data standards?
• Are shadow systems currently covered under your trust's Cyber Security policies and IG Toolkit?
Note – If in answering any question you believe that the answers would breach section 35 please provide that information you are able to.

It Is imperative that the Trust is cyber resilient, cyber-attacks against infrastructure have the potential to inflict significant, real-life disruption and prevent access to critical services that are vital to the functioning of Trust systems.

The Trust is required to balance whether the information requested is in the public interest (the public as a whole) and if the release of such information would have the potential to cause any harm should that information get into the wrong hands.

Cyber security is a real threat to organisations and as such The Dudley Group has to provide assurance as part of the Data Security and Protection Toolkit and to its patients that it undertakes assurance and IT vetting against all its systems to offer Cyber Assurance - Confidentiality , Integrity and Availability (CIA) and security of clinical and nonclinical systems used by the Trust, Privacy By Design - Incorporating, Privacy Legislation , General Data Protection Regulation Compliant systems and IT Vetting - ensuring compliance with other mandatory requirements e.g. Clinically fit for purpose and safe patient systems; Data Security and Protection Toolkit (DSP Toolkit) compliant; NHS Improvement, NHS Digital and other regulatory body required standards for IT systems.

For the Trust to offer this assurance it is imperative that information about it systems is not offered into the public domain. Information of this type could potentially allow unscrupulous persons to 'hack' into critical health systems and information which would cause detriment to it patients and staff.
Patching information for systems is widely available in the public domain, thus informing the general public of systems vulnerabilities enabling them the opportunity to try and attack any potential vulnerabilities.

As assurance The Trust is ISO27001 and Cyber Essentials certified due to the resilience it places on its vetting and assurance. https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

Exemption (43) has been applied given it is commercially sensitive in that providing this information may compromise information security.